

Proceedings



21st IEEE Computer Security Foundations Symposium

CSF 2008

23-25 June 2008 • Pittsburgh, Pennsylvania



Los Alamitos, California
Washington • Tokyo



Proceedings



CSF 2008

Table of Contents

Preface	viii
Committees	ix

Language-Based Security

Language Based Secure Communication	3
<i>Michele Bugliesi and Riccardo Focardi</i>	
Refinement Types for Secure Implementations.....	17
<i>Jesper Bengtson, Karthikeyan Bhargavan, Cédric Fournet, Andrew D. Gordon, and Sergio Maffei</i>	
A Trust Management Approach for Flexible Policy Management in Security-Typed Languages	33
<i>Sruthi Bandhakavi, William Winsborough, and Marianne Winslett</i>	

Security Models in Theory and Practice

Hyperproperties	51
<i>Michael R. Clarkson and Fred B. Schneider</i>	
Security Decision-Making among Interdependent Organizations	66
<i>R. Ann Miura-Ko, Benjamin Yolken, John Mitchell, and Nicholas Bambos</i>	

Declassification and Erasure

Tractable Enforcement of Declassification Policies	83
<i>Gilles Barthe, Salvador Cavadini, and Tamara Rezk</i>	

End-to-End Enforcement of Erasure and Declassification	98
<i>Stephen Chong and Andrew C. Myers</i>	

CSF/LICS Joint Invited Talk

Cryptographically-Sound Protocol-Model Abstractions	115
<i>Christoph Sprenger and David Basin</i>	

Authorization Logic I

An Authorization Logic with Explicit Time	133
<i>Henry DeYoung, Deepak Garg, and Frank Pfenning</i>	

Authorization Logic II

DKAL: Distributed-Knowledge Authorization Language	149
<i>Yuri Gurevich and Itay Neeman</i>	

Access-Control Policies via Belnap Logic: Effective and Efficient Composition and Analysis	163
<i>Glenn Bruns and Michael Huth</i>	

Evidence-Based Audit	177
<i>Jeffrey A. Vaughan, Limin Jia, Karl Mazurak, and Steve Zdancewic</i>	

Protocol Analysis I

Automated Verification of Remote Electronic Voting Protocols in the Applied Pi-Calculus	195
<i>Michael Backes, Cătălin Hrițcu, and Matteo Maffei</i>	

Specifying Secure Transport Layers	210
<i>Christopher Dilloway and Gavin Lowe</i>	

Towards Producing Formally Checkable Security Proofs, Automatically	224
<i>Jean Goubault-Larrecq</i>	

Composition of Password-Based Protocols	239
<i>Stéphanie Delaune, Steve Kremer, and Mark Ryan</i>	

Cryptographic Foundations

Computational Soundness of Symbolic Zero-Knowledge Proofs
against Active Attackers.....255
Michael Backes and Dominique Unruh

Joint State Theorems for Public-Key Encryption and Digital Signature
Functionalities with Local Computation.....270
Ralf Küsters and Max Tuengerthal

Information Flow and Concurrency

A Type System for Observational Determinism.....287
Tachio Terauchi

Information Flow in Systems with Schedulers301
Ron van der Meyden and Chenyi Zhang

Protocol Analysis II

A Correctness Proof of a Mesh Security Architecture.....315
*Doug Kuhlman, Ryan Moriarty, Tony Braskich, Steve Emeott,
and Mahesh Tripunitara*

Formal Analysis of PKCS#11331
Stéphanie Delaune, Steve Kremer, and Graham Steel

Author Index345